Inf Syst Front (2016) 18:1251–1263
DOI 10.1007/s10796-015-9572-3

Understanding governance, risk and compliance information systems (GRC IS): The experts view

Anastasia Papazafeiropoulou[1] · **Konstantina Spanaki**[2]

Published online: 23 June 2015

Abstract Although Governance, Risk and Compliance (GRC) is an emerging field of study within the information systems (IS) academic community, the concept behind the acronym has to still be demystified and further investigated. The study investigates GRC systems in depth by (a) reviewing the literature on existing GRC studies, and (b) presenting a field study on views about GRC application by professional experts. The aim of this exploratory study is to understand the aspects and the nature of the GRC system following an enterprise systems approach. The result of this study is a framework of particular GRC characteristics that need to be taken into consideration when these systems are put in place. This framework includes specific areas such as: goals and objectives, purpose of the system, key stakeholders, methodology and requirements prior to implementation, critical success factors and problems/barriers. Further discussion about the issues, the concerns and the diverse views on GRC would assist in developing an agenda for the future research on the GRC field.

Keywords Governance, Risk and Compliance Information Systems (GRC IS) · Enterprise Systems · System Aspects

✉ Anastasia Papazafeiropoulou
anastasia.papazafeiropoulou@brunel.ac.uk

Konstantina Spanaki
k.spanaki@imperial.ac.uk

[1] Department of Computer Science, Brunel University, London, St. Johns building, Uxbridge UB8 3PH, UK

[2] Imperial College, London, Tanaka building, South Kensigton campus, London SW7 2AZ, UK

1 Introduction

The Sarbanes-Oxley Act (SOX), Basel II and the other international and regional regulatory mandates resulted in the expansive adoption of GRC software systems. Given the complex regulatory burden imposed upon both executives and IT administrators, the tools provided by GRC software vendors became increasingly important in meeting the new standards. GRC software enables an organization to manage the GRC-related enterprise strategy following a holistic approach. A single framework is provided integrating the three aspects of GRC acronym together, supporting the administrators in monitoring and enforcing rules and procedures. Successful implementations of single integrated GRC software packages enable organizations to manage risk, reduce costs incurred by multiple installations and minimize complexity for managers.

GRC acronym stands for Governance, Risk and Compliance as an integrated concept and describes different organizational activities, from arranging an annual audit to the establishment of internal continuous control monitoring procedures, to setting up roles and responsibilities in business processes and the system users, to data analytics procedures. The term GRC was initially introduced in 2004 by PricewaterhouseCoopers and since then is becoming a widely spread and important emerging solution for the business requirements of an organization (Gill and Purushottam 2008). Organizations usually adopt GRC systems, as another integrated application to their existing systems, however other GRC implementations follow another approach which comprises a whole GRC strategy; reorganizing the whole enterprise environment in order to follow a proactive reaction to GRC principles. Most large organizations world-wide have already adopted GRC software, and also small and medium sized enterprises (SMEs) are interested lately in following the integrated GRC approach fostered by GRC systems.

Though GRC integrated systems have only become available in recent years, GRC principles were always followed by organizations by either manual processes or by using non-integrated software solutions. Nonetheless, until recently, academic research on the integrated GRC initiative was not extensively developed despite its significance for the organizations (Racz et al. 2010c). A special issue in Information Systems Frontiers in April 2012 shows the interest of the IS community in understanding GRC systems better (Sadiq et al. 2012). Existing literature about GRC indicates that IS researchers have more ground to cover in this field, as a lot of aspects have not been investigated yet. The literature of GRC systems was developed through the past few years; however a common understanding about the nature and the definition of GRC as an information system (IS) is still not completely clear yet.

While the literature refers to the GRC topic including different views regarding the perspective, which is analyzed (financial GRC, enterprise GRC, GRC IS etc.); the study herein takes GRC as an enterprise information system and investigates it as an integrated software solution building the GRC landscape within the enterprises. This study focuses on the need to analyze further the GRC system aspects and define the GRC software as an enterprise system.

Given the diversity of the opinions about GRC, the study will follow two sources of evidence. Initially a literature review will explore the academic research on GRC as an integrated system, and in the second part a field study in the area of GRC will explore the characteristics of the systems by interviewing professionals with experience in the use and adoption of GRC systems.

2 The GRC concept and frameworks

Recent studies on GRC have highlighted the lack of scientific research in integrated governance, risk and compliance (Racz et al. 2010b). While the area of GRC implementations has been an emerging one, especially within the last few years, most of the frameworks developed so far cannot give a clear view of integrated GRC and specifically the implementation of it. Furthermore, these frameworks cannot provide a roadmap for the organizations with regard to the GRC implementation process and how they can strategically benefit by aligning GRC technological infrastructure with their business objectives. A few frameworks were identified presenting models with reference to integrated GRC solution.

As it was mentioned above, there was a special issue of Information Systems Frontiers on the GRC IS topic which contributes to a wide range of Governance, Risk and Compliance areas, from the adoption of compliance management systems to the automated checking of process compliance. (Sadiq et al. 2012). The same issue includes a longitudinal case study to explore the use of information systems for risk management in the utility sector (Scott and Perry 2012). The main focus of this study is reporting on risk management practices and the identification of related best practices in energy sectors and if this can be expanded in a general approach it can crucial for the advancement of GRC practices (Sadiq et al. 2012; Scott and Perry 2012). Gangadharan et al. (2012) propose a solution to a compliance problem in the space of software licensing (Gangadharan et al. 2012), this approach adopts the Open Digital Rights Language for checking compatibility of free and open source software licenses and mostly focuses on compliance issues.

Hoffmann et al. (2012) suggests the deployment of executable process models by asserting their compliance to a set of rules. More specifically, this paper introduces a semantic annotation approach for process models and the ability to model preconditions and effects of tasks within a process (Hoffmann et al. 2012). A theory-based model of effective IT governance is presented in the same issue as well as the discussion of the outcomes of the empirical testing of this model and it focuses more on governing outsourcing relationships (Ali and Green 2012). At the same issue Ly et al. (2012) discuss the requirements that must be met by process management systems to support semantic constraints and the criteria that enable integrated compliance support through the entire process lifecycle through Semantic Technologies approaches (Ly et al. 2012). A research by Butler and McGovern analyse environmental compliance Information Systems and they propose a framework for the design of environmental compliance management systems (Butler and McGovern 2012). This research focuses on the GRC in the environmental management area. The last paper of the GRC special issue closes with a modelling approach of risks and a process for the assessment of IT risks (Strecker et al. 2011).

The Open Compliance and Ethics Group (OCEG) presents the OCEG Capability Model GRC360 which consists of nine categories and 29 sub-elements for each of which sub-practices are listed (Racz et al. 2010a; OCEG 2007). The model gives an insight to GRC practices and activities; however it does not distinguish between operative and managerial processes (Racz et al. 2010a). Mitchell (2007) also proposes a framework to drive "principled performance" which is basically the very early stage of GRC360 Capability Model (Mitchell 2007). The OCEG Capability model is also discussed by Rasmussen (2009) who refers to the "Enterprise view of Risk and Compliance" and proposes OCEG Capability Model as an Enterprise Architecture for GRC (Rasmussen 2009).

Paulus (2009) on the other hand, describes "GRC Reference Architecture" with a model which consists of four major phases:

a) requirements modelling
b) status investigation

c) situation improvement
d) crisis and incident management

This model is easy to understand (Paulus 2009), however it does not include in-depth analysis and insights into the implementation of GRC. The "Strategic Framework for GRC" (Frigo and Anderson 2009) describes the 'risk policies and appetite' and these set overall common goals for adding value and protecting the common processes associated with GRC practices. It can strategically help organizations to manage their GRC initiatives; however the framework mixes processes with organizational entities and objectives and sometimes can be difficult to follow especially for enterprises not very familiar with the GRC landscape (if they are at their early stages of risk management).

The GRC system solution is also proposed by Dameri (2009), however in this research study an in-house developed system approach is followed. The study presents the Enterprise Information Management Systems (EIM) architecture supporting GRC developed in different enterprises (Dameri 2009).

Tapscott's (2006) approach to GRC gives four core values for the enterprises to achieve the 'trust' expectation, which is their main aim when they take an integrated approach to GRC. This approach (Tapscott 2006) although it is easy to follow, does not translate its four core values into a process model that would help enterprises take a wider view of their GRC activities. Another research, conducted by PricewaterhouseCoopers (2004) develops an Operational Model for GRC; however this model also mixes in each of the four steps which it is consisted of, the organizational entities, activities and the relationships involved within these steps. This Operational Model (PricewaterhouseCoopers 2004) combined with the four core values as presented by Tapscott (2006) could develop essential tools for the GRC implementation process analysis.

Wiesche et al. (2011) present a GRC framework by linking GRC to Accounting Information Systems the result of which is the "Framework for GRC IS Value Drivers". This framework (Wiesche et al. 2011) is taking an isolated accounting perspective of GRC and not an enterprise-wide approach. Furthermore, Racz et al. (2010b) translated the GRC definition to a "Frame of reference for GRC Research" which depicts the definition into a figure and is the basis for the research in the GRC field (Racz et al. 2010b).

A framework for GRC is also presented by Gericke et al. (2009). The core aim of this framework is to analyze the GRC implementation with situational method (Gericke et al. 2009) while identifying the method fragments. The method fragments are divided into five categories: conceptual, strategic, organizational, technical and cultural. The basis for this research is the GRC solution rollout, rather than the successful implementation of the GRC software. This framework can be used for the development of the analysis framework for the integrated GRC implementation. More recent research in the field of integrated GRC includes the "Conceptual Model for Integrated Governance, Risk and Compliance" by Vicente and da Silva (2011) which presents the concepts and the key functions of GRC by using OCEG Capability Model (2009, http://www.oceg.org). The Conceptual Model can be used for the better understanding of GRC integration and as a tool for structuring the analysis framework of integrated GRC implementation process. Table 1 below gives an overview of the literature on GRC systems and their specific focus.

The above analysis shows that the current literature on GRC systems is primarily concerned with the technical/instrumental application of GRC systems while there is lack of understanding of the true nature of these systems as well as their role in the organizational life. Thus, in the next section we present a field study where practitioners from the area of enterprise systems and GRC in particular express their views on the application of GRC systems and their particularities as a type of enterprise system specialized in IT based on governance, risk management and compliance.

3 GRC IS field study: Taking the experts view

This section will include the description of the field study conducted for the GRC implementation. The section includes information about the sample and the data collection process, as well as the data collected through the interviews.

3.1 Methodology

The research followed an interpretive philosophical research stance (Klein and Myers 1999). The reason for this choice is that there are wide areas of social, political, and cultural issues related to the success of the GRC implementation process. Therefore, the study of the GRC implementation process cannot be separated from its organizational and cultural context. Another reason is also the fact that interpretivism allows concepts to emerge from field data rather than using preconceived theories from the field (Miles and Huberman 1994). Therefore, the study of the GRC Implementation cannot be separated from its organizational and cultural context. The enterprise value drivers that will be investigated cannot be separated from the GRC implementation setting as they are influencing the whole GRC implementation process and should be considered in order to identify and analyze them effectively.

The research followed a field study approach and aimed to get insights on the implementation and use of GRC systems in organizations. More specifically, the first phase of the investigation involved the development of general knowledge about the GRC IS implementation. The literature review of the field assisted in the identification of the key stakeholders

Table 1 Existing literature on GRC systems

Author	Year	Description	Focus
PricewaterhouseCoopers	2004	A four steps model, as well as organizational entities, activities and the relationships involved within these steps	An Operational Model for GRC
Tapscott	2006	Four core values for the enterprises to achieve the 'trust' expectation, which is their main aim when the take an integrated approach to GRC	Four core values approach
Mitchell	2007	A framework to drive "principled performance"	The very early stage of GRC360 Capability Model
Open Compliance and Ethics Group (OCEG)	2007	The OCEG Capability Model GRC360 which consists of nine categories and 29 sub-elements for each of which sub-practices are listed	Insight to GRC practices and activities
Dameri	2009	An in-house developed GRC application	EIM systems architecture
Rasmussen	2009	The "Enterprise view of Risk and Compliance" and the OCEG Capability Model as an Enterprise Architecture for GRC	The Enterprise Architecture for GRC
Paulus	2009	A model, which consists of four major phases: a. requirements modelling, b. status investigation, c. situation improvement, d. crisis and incident management.	GRC Reference Architecture
Frigo and Anderson	2009	The 'risk policies and appetite' approach and these set overall common goals for adding value and protecting the common processes associated with GRC practices	Strategic Framework for GRC
Gericke et al.	2009	A framework for GRC with the core aim to analyze the GRC implementation with situational method while identifying the method fragments. The method fragments are divided into five categories: conceptual, strategic, organizational, technical and cultural	The GRC solution rollout
Racz et al.	2010b	A figure definition, which is the basis for the research in the GRC field.	Translated the GRC definition to a "Frame of reference for GRC Research"
Wiesche et al.	2011	The "Framework for GRC IS Value Drivers" which is about the accounting aspects of GRC and not an enterprise-wide approach.	A GRC framework linking GRC to Accounting Information Systems
Vicente and da Silva	2011	Concepts and the key functions of GRC by using OCEG Capability Model (2009)	"Conceptual Model for Integrated Governance, Risk and Compliance"
Strecker et al.	2011	A modelling approach of risks and a process for the assessment of IT risks	'RiskM: a multi-perspective modeling method'
Scott and Perry	2012	Reporting on risk management practices and the identification of related best practices in energy sectors	'A longitudinal case study for the use of information systems for risk management'
Gangadharan et al.	2012	Adoption of the Open Digital Rights Language for checking compatibility of free and open source software licenses and mostly about compliance issues.	'An approach to a compliance problem in the space of software licensing'
Hoffmann et al.	2012	The deployment of executable process models by asserting their compliance to a set of rules	'A semantic annotation approach for process models'
Ali and Green	2012	A theory-based model of effective IT governance and the discussion of the outcomes from the empirical testing of this model	'A model for governing outsourcing relationships'
Ly et al.	2012	The process management systems to support semantic constraints and the criteria that enable integrated compliance support through the entire process lifecycle	'Semantic Technologies approaches for process management'
Butler and McGovern	2012	Analysis of the GRC compliance Information Systems in the environmental management area	'A framework for the design of environmental compliance management systems'
Yu et al.	2013	An IT internal control framework with enterprise-wide perspective embraced administrative, technical and physical internal control reinforcement.	"IT GRC-based Internal Control Framework"
Asprion and Knolmayer	2013	Institutional pressures and quality aspects affecting the assimilation of compliance software in post-implementation period of GRC	"A model for the Assimilation of Compliance Software"
Nissen and Marekfia	2013	Current research on the basis of strategic GRC-Management requirements	"A research agenda for the GRC area"
Spanaki and Papazafeiropoulou	2013	Primary analysis of the GRC implementation process	"An analysis framework for the GRC implementation process"
Nissen and Marekfia	2014	GRC models already existing in the GRC literature and highlight the aspects to be considered in terms of an integral approach.	"Data-Centered Conceptual Reference Model for Strategic GRC-Management"

of this process as well as the GRC characteristics drawing from the data coupled with the theoretical background (Fig. 1). Initially, the GRC IS implementation project stakeholders were identified by Gericke et al. (2009) as: a) Project Manager, b) GRC Expert, c) Top Management and d) IT Consultant. These four categories were also used as interviewee groups, in order to choose the stakeholders from different categories and investigate a variety of viewpoints. The first phase also assisted in gathering data for the development of the interviews for the second phase. The second phase included further investigation about the GRC IS characteristics. The GRC stakeholders were interviewed about the system's characteristics in specific; and how these influence the success of the GRC IS implementation projects.

The field study investigation chose different groups of GRC stakeholders and more specifically stakeholders involved in more than three GRC implementation projects worldwide in the last decade. The names of the interviewees were changed for reasons of confidentiality and anonymity. The interviews with the project stakeholders (lasted about an hour each) were transcribed. The secondary data from the organization's web site and publically available sources as well as from the implementation company's publically available resources contributed to the data collected from the interviews at this stage. The method used for the analysis of the interviews at the first stage was thematic analysis as proposed by Boyatzis and Braun and Clarke (Braun and Clarke 2006; Boyatzis 1998). The identification of the GRC IS characteristics was developed through the coding of the interview data (the interviews conducted in the first phase of the investigation) coupled with the literature investigation of the area.

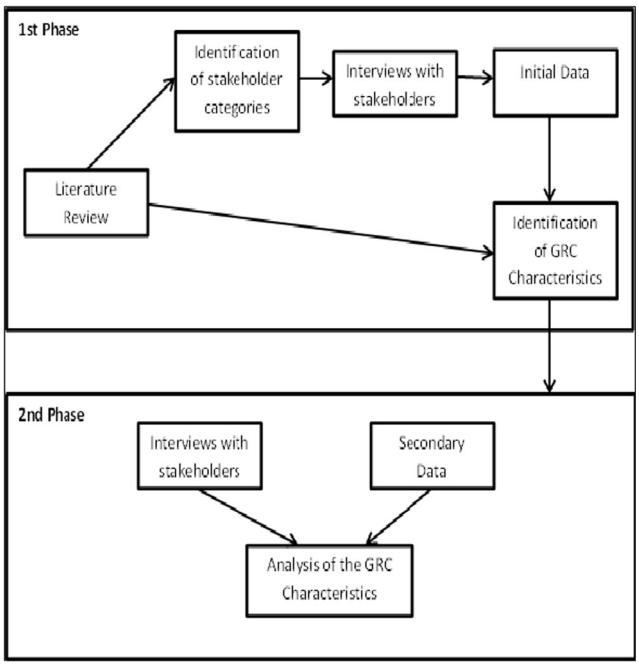

Fig. 1 The 2 phases of the research

The second phase involved interviews with the GRC stakeholders, in order to confirm if the initial findings about the GRC IS implementation and investigated in specific the characteristics as these were arising from the literature and the dataset of the first phase. More specific the aspects of the GRC IS identified in the previous phase; were enhanced from the information provided through the interviews coupled with the literature sources. The final findings of the two phases comprise the identification of the characteristics of the GRC IS implementation and their analysis.

3.2 Thematic analysis of the data

The empirical setting of the interviews builds upon the broad understanding and experience of people (stakeholders) involved in GRC IS implementation projects in the first phase of the investigation, more specifically; the focus of selection of the interviewees was on maximizing the diversity. By maximizing the diversity, the sample will provide different and varying data. The research shares the GRC IS implementation process as a common unit of analysis, but uses different roles within the implementation projects as contexts. The qualitative data analysis was conducted in 16 stakeholder interviews, and the results of this analysis were confirmed at the end of the each of the two phases. The data from the interviews conducted were analysed through the phases of thematic analysis as described by Braun and Clarke (2006). More specifically, the thematic analysis was conducted following the following steps (Braun and Clarke 2006; Boyatzis 1998):

- **Step 1 (Familiarising with the code):** The interviews were recorded and transcribed, and the researchers were familiarising with the transcripts of the interviews.
- **Step 2 (Generating initial code):** The researchers investigated initial emerging codes from the transcripts of the interviews
- **Step 3 (Searching for themes):** The emerging areas from the transcript were identified and matched to the theoretical background, and the themes were developed
- **Step 4 (Reviewing themes):** The themes were reviewed and confirmed by the interviewees
- **Step 5 (Define and naming themes and sub-themes):** Themes and sub-themes were defined and developed in the final form.
- **Step 6 (Producing the analysis):** The analysis of the themes and sub-themes followed

In order to achieve diversity of the sample, the research included a broad range of roles in the GRC IS implementation projects as these are related to GRC roles. Since the different roles within the GRC IS implementation provide different focal points, the interviews were two for each stakeholder group for covering different roles using mixed purposeful

sampling. The stakeholders were working for different implementation projects and they have experience between 5 and 10 years in the implementation projects of these specific systems. The companies they work are based in the UK and they had experience in implementation projects worldwide. Table 2 provides the details of the participants role in the projects as well as their experience and time spend with the researcher. The second phase also was based on the methodology of field studies. The methodology of the second phase followed the same approach as this was described for the first phase. The analysis was conducted after each of the two phases of data collection and aimed to get insights on the implementation process of GRC software initiatives.

The roles included in Table 2 are analyzed as follows. A project team, is headed by a *project manager*. The project manager coordinates the project and gives directions for the whole implementation process and the activities involved; therefore, the project management role is crucial for GRC implementations. The *GRC expert* specializes in all the areas of the GRC IS. The support provided is within the scope of the expertise for the processes implemented. The expert is also responsible for the integration of the relevant business processes within the system. The *top manager* is responsible for the development of the project strategy; and to support the strategy that will be followed during the whole project. The *IT consultants* are responsible for the integration of the system with the organizational environment of the enterprise. Moreover, they will give training and directions to the IT unit of the enterprise for using the new implemented system.

4 Data analysis

The second phase of the investigation included interviews about the GRC implementation aspects. The main output of the second phase was a brief analysis of the GRC implementation aspects. The target group interviewed about these aspects was professionals who had experience in GRC implementation projects (GRC implementation stakeholders as these were described by Gericke et al. (2009). The interviews were consisted with questions about:

(a) the goals and objectives of these projects,
(b) purpose of the system and key stakeholders
(c) requirements prior the implementation,
(d) critical success factors,
(e) problems/ barriers throughout the implementation process.

4.1 Organizational goals and objectives for the GRC implementation

The stakeholders of the GRC implementation projects discussed the major goals and objectives of a GRC implementation project. These goals and objectives usually lay within the financial reporting and controlling scope. The discussion of this scope lead to decisions about implementing a system that can support the continuous control monitoring needs of the enterprise, as the interviewees explained the need of IT software for the enterprise controlling strategy seems most of the times as a crucial issue:

> '*The usual scenario is that a company has an annual audit, and the typical audit point which comes back to ERP systems. […] Therefore, the companies do not have any kind of GRC tool to monitor the risks in any way, to address that annual audit point. That is the point when they realize: ''OK we need some sort of compliance tool*"' (IT Consultant 1)
>
> '*It is very challenging when the stakeholders are driven by an audit, and they decide to implement a new piece of software for auditing and controlling. At this case you have to communicate the requirements and bring all the teams together on-board*' (GRC Expert 1)

The stakeholders also discussed the goal of efficient and effective business operations, which leads enterprises to

Table 2 Project roles and interviewees of the second phase

Participant ID	Length of 1st phase	Length of 2nd phase	Length of confirmation	Experience
GRC expert 1	1 h 25 min	1 h 25 min	0 h 28 min	8 years
GRC expert 2	1 h 05 min	1 h 45 min	0 h 15 min	9 years
GRC Project Manager 1	1 h 40 min	1 h 40 min	0 h 22 min	10 years
GRC Project Manager 2	1 h 55 min	1 h 15 min	0 h 32 min	7 years
Top Manager 1	0 h 45 min	0 h 45 min	0 h 16 min	6 years
Top Manager 2	0 h 35 min	1 h 05 min	0 h 23 min	5 years
IT Consultant 1	1 h 45 min	1 h 45 min	0 h 27 min	5 years
IT Consultant 2	1 h 48 min	1 h 36 min	0 h 21 min	5.5 years

implement GRC systems. There are so many cases when the businesses are helpful with the GRC implementation plan. These cases are mostly when they are looking for ways to be more proactive in terms of user access, process automation and improving their processes. If they are driven by an audit to the GRC implementation, the case becomes more challenging, as it was mentioned from the professionals during the interviews. The better operational performance goal was discussed as it is also stated below:

> *'From a strategic point of view, they want to have better operational governance. They want to be informed about the people and their roles, to have accountability and define the responsibilities in the organization, for running better business processes and work more efficiently'* (Project Manager 1)
> *'On a risk management side, they want their strategic goals to be likely to identify key performance related to risk, and have the processes in place to mitigate those risks'* (Project Manager 1)

A third goal for the GRC implementation that was discussed through the interviews was the compliance with the laws and regulations. The third goal of compliance is often seen in audits, but it is more than that. Regulations are part of that compliance; there are regulations as Sarbanes-Oxley, Basel II, holistic standard FDA etc. However, there is also compliance to standards the organizations set up internally.

> *'If you have processes for risk management and if you have processes for governance, so is compliance to them as well. You have to measure the activities to be able to say that they are operating effectively. Therefore, compliance goes to its regulatory audits, but also compliance to internal procedures'* (GRC expert 1)

The previous quotes from the interviews identified the goals and objectives of the GRC implementation. These goals usually lay within the 'finance' umbrella, where financial reporting and controlling play an important role. The enterprises within the last decade became more conscious regards controlling and monitoring practices and seek for a tool to assist them with the auditing controlling practices. Another ambition can be described as the strategic plan of the organizations that follows practices of more efficient and effective business operations, therefore there is a need for a software which provides a clear view of the enterprise (user access, the roles and the business processes). The third goal for implementing GRC software within the enterprise includes the compliance with the internal and external regulatory standards.

4.2 Purpose of the system and key stakeholders

As it is also stated in the previous arguments, the GRC implementation is risk management, control monitoring, and information sharing oriented. Additionally, the interviewees were asked about the GRC implementation key stakeholders. The interviewees related the stakeholders to the following categories:

1. project manager
2. GRC experts
3. Finance team
4. Audit team
5. IT team
6. consultants
7. GRC Systems vendor
8. project team members

These key stakeholder categories are influencing the GRC implementation process, therefore their roles, activities and interests should be further investigated.

The above stakeholder categories for the GRC implementation can also be matched with the four groups of stakeholders that were identified from the literature in order to facilitate the initial participant selection process. The first six categories bare similarities with the stakeholders-GRC implementation interviewee categories, as these were identified by Gericke et al. (2009).

The project manager and GRC expert roles are the same in both categorizations; the top managers are substituted with the finance and audit teams, that have very basic top management roles at the GRC implementation; and the IT consultants can be matched with the IT team and consultants. The GRC systems vendor, project team members are categories of stakeholders involved in the GRC implementation, as these were identified from the interview data; however they were not presented at the literature review initial identification process. These two categories have important roles in the GRC implementation; however, the key stakeholders for the implementation are the first six categories, as they are the core members of the GRC implementation project.

4.3 Practices prior the GRC implementation

While discussing the methodologies and practices before the decision of the GRC implementation, the interviewees were mostly discussing non-automating strategies the enterprises followed. These strategies can be used as frameworks for the GRC implementation. Enterprises usually operate a non-automated strategy for GRC practices before the implementation of the software. These manual, non-automated practices can set the initial framework to start with the GRC system implementation. Initially, there is a need to define the

processes and set the organizational objectives. At this stage, the companies are well prepared in order to start efficiently with the implementation as the GRC professionals discussed.

'GRC software is not a tool that you can pick up off the shelf, you go and implement it and everything is fixed. To get an understanding about what available controls you want to be improved and have that governance structure, get everybody thinking in the right lines. And then what you are doing is you plug in the technology solutions into that framework to address that' (Project Manager 1)

While discussing the methodologies that were used before the implementation of a GRC tool within the enterprises, the point that was addressed was the fact that the GRC software is not a technological tool that can be plugged in the organization without a prior business framework. It is necessary to develop a plan about the available controls, the governance structure, and the business objectives, in order to implement successfully the new technology.

'GRC technology provides a strict tool. You cannot implement such a strict tool in an organization that does not already operate some form of controls already (manual or with the use of other technologies)' (GRC expert 1)

'The organization should be prepared before the implementation. If you go and implement the tool without having any prior business experience in a control environment, that implementation is going to fail from the start' (IT Consultant 1)

The GRC tool as it was noted from the interviews, is a strict controlling tool, therefore there is a need of a 'preparation' for the organization seeking to implement such a technology. There is a requirement for a prior controlling framework within the enterprise; the enterprise needs to work under some controlling processes, either manually or with the assistance of other tools. The organization cannot implement the GRC tool if there is no prior GRC policy and processes, as the GRC environment will be very strict if the organization does not already used to operate a model of controls.

The organizational and technical requirements for a GRC implementation should be considered very carefully, as it was also discussed throughout the interviews with the GRC stakeholders. The stakeholders were asked about the GRC requirements; and highlighted the importance of each of these requirements. The first three technical and organizational aspects that were developed during the interviews can be grouped in the following categories: the development of the business case, the identification of the risks, the project planning (how the system will be rolled out, supported, maintained and upgraded). These topics were discussed as follows:

'[…] Key people will identify the risks from an operational side, as well as train the people inside the organization to be able to manage the tool the project team will also develop the project plan, about the system rollout, and how it can be supported and maintained.' (IT Consultant 1)

From a business perspective, the requirements are based on the fact that the organization can support such a system. The organization needs to have the processes in place in order to be able to identify the risks and the tools for articulating these risks. The business case should be developed from the initial stages of the GRC implementation project; identifying the risks that will be plugged in the system and defining their requirements. While being early informed for the risks, the project plan should be also defined in order to understand how the system would be rolled out, supported, maintained and upgraded. Other requirements emphasized throughout the interviews, were described as the need for a change management plan, budget planning and clearly the decision to proceed with the plan.

'Definitely, as in every IT implementation project, you need to have a change management plan, as well as the business plan. Also, thinking about what budget you want to spend at such an implementation will affect most of the choices that will be taken later into consideration' (Project Manager 1)

Another point that was brought to the fore from the interviews was the identification of the roles and who owns each risk; controls their content and approve those risks. Additionally, a topic that was discussed was the significance to develop a current state analysis; more specifically the need the enterprise to provide a current GRC framework to start with.

'There is a need of the technical infrastructure as well as a current state analysis, in order to identify the GRC framework to start with. This part is very crucial' (GRC Expert 1)

'You need to know also what systems are in place, what you need to connect with the GRC system, because this affects who is going to have access in what and what are the roles in each of the existing systems. You need to know who owns each role, who controls the content of them and who approves those risks' (IT Consultant 1)

The selection of software and software vendor and the IT infrastructure of the organization is another requirement. This

requirement included the IT landscape of the organization; and more specifically what systems they use. Usually, large enterprises decide to implement the GRC systems; the SMEs are not very interested in such tools, according to the interview data.

'There are different 'sizing' options for these systems; this is called 'T-shirt sizing' and they are 'Small, Medium and Large'; each one fits in different enterprises, and they are dependable to the size of the organization' (GRC expert 1)

'Larger enterprises require different technical aspects of the system. […] So the vendor and the software selection is one of the basic technical requirements of a GRC implementation' (Top Manager 1)

The requirements from an organizational and technical perspective were stated in the discussions with the stakeholders and they were characterized as critically important as the phase before the actual software implementation can indicate the whole implementation project success.

4.4 Critical success factors for the GRC implementation

The critical success factors of the GRC implementation were identified in the interviews with the stakeholders and they are described mostly in the following points. Initially, the project should ensure a top management support; coming from the system manager or a business sponsor. While the top management support is important, the key stakeholders should be also involved; these stakeholders should be both from IT and financial-auditing teams, that should be engaged to communicate effectively for the success of the project. One of the most important parts for the implementation of these tools is the achievement of a common understanding about the need of a GRC solution. The reasons for implementing a GRC system are mostly finance-led. The organizations need to identify the finance and operational risk in their systems.

'All the key stakeholders are sitting under the 'finance-umbrella', so if you don't engage the finance people of the organization in this project, the project will have no success' (Project Manager 1)

'One of the largest challenges of the GRC implementation is the communication between the stakeholders. Usually, the preferred method is to catch some management sponsorship that will help also to achieve a common understanding about the need for such a solution' (GRC Expert 1)

Furthermore, information should be cascaded throughout the organization improving various functions (regards information risk, internal audit, user provisioning, business process ownership). The Identification of the process owners and the risks associated with it will be another challenge for the implementation tasks.

'The 'ultimate' sponsorship will be able to cascade information throughout the organization improving various functions. The key to implement GRC, you have to know who owns that process and who owns a new risk associated with it' (IT Consultant 1)

'The important thing is not so much the risk rule sets; this is kind of a generic thing, but the identification of the process owners, the roles and the risks. The business should consider how things work' (Top Manager 1)

Other factors discussed were about defining the GRC system requirements and the training of internal people to be able to manage the system and cope up with the solutions. The last point was highlighted with great importance as solving the problems internally will avoid further risks from the organization. A critical point for the implementation is to define early the system requirements and follow a project plan, which clearly states these requirements.

'The organization should get involved also with the provisioning workflows, in order to understand how things work. So for example, they might think 'yes we have the role in this stage, but we do need the risk in this stage'. The role owner is the same person as the risk owner, so rather than approving the request, twice it makes more sense to do everything in a single stage. You need to train them and get them involved in the project' (IT Consultant 1)

'You have to train the internal people to be able to manage and cope up with the solutions. It is exactly much the same as implementing any module of ERP. You have to have people knowing the system and knowing 'why'. As for technical people it is very easy to teach them how to do something, but understanding is the biggest challenge' (GRC Expert 1)

The above factors are critical in order to ensure a successful GRC implementation process. The critical success factors identified for most of the ES implementation projects (in the previous section), can be also employed additionally in the case of the GRC implementation as well. However, the GRC systems have also additional factors to consider as well.

4.5 Problems/barriers of the GRC implementation

Another topic for discussion during the 2nd phase of the investigation was the problems and the barriers that the stakeholders may face throughout the GRC implementation

project. The stakeholders highlighted in this part of the interviews, the following issues that may affect the project.

The technical complexity of the solutions that requires a great deal of expertise can be a challenge itself. Experienced project teams should implement such complex systems in order to avoid common problems due to their complicated nature. Also, if the company is not ready for a GRC solution that will introduce a further challenge for the whole project as the people of the organization need to understand why they need it and what solution they need to implement.

'The main issues affecting the GRC implementation are two: technology and people. The first is mostly because GRC systems are complex systems that require great deal of expertise. The second usually occurs because the people within the company are not ready for such a tool; they do not know why such a software is required and they do not also know what type of software to implement' (Top Manager 1)

A big problem exists also when there is no control framework already in the organization and the project team needs to develop a control framework from scratch. In that case, the organization does not have that level of detail already and cannot put a 'stricter' tool as GRC solutions. The organization should be 'mature' enough with a level of controls already inside the business landscape.

'One of major success factors is the control frameworks that already exist in the organization. If there is no control framework already in this organization, there will be a great problem. The problem exists as the organization does not already have that level of maturity regards controlling functions, therefore the implementation of a strict controlling tool as GRC will be very difficult to adopt in such unstructured business environment' (GRC Expert 1)

Another common challenge for all the implementation projects that will be faced also in a GRC project is the conflicting priorities within the organization (between the stakeholders). Therefore, the need to have a strong project manager in order to avoid the 'conflicting priorities' issue seems as really important. This project manager will bring all the teams together to work to ensure the success of the GRC project.

'Within the organizations in most cases there are conflicting interests and priorities for the GRC system. They have also different understanding of the system and objectives as well' (IT Consultant 1)

The vendor selection was identified as a critical success factor in a previous section; however there are a lot of times that a complicated GRC solution is selected, and that provides additional problems as this solution could be difficult to work in the organizational landscape.

'The system complexity is a factor that can affect the implementation; also it can make difficult the process of customization as well a system configuration. The software selection is very important for identifying which system suits better in your organization, the system should be not very complicated otherwise the organization will have problems later' (GRC Expert 1)

The training of the IT team is an important stage, however in cases that the IT team of the organization is not trained on the system and they rely on external consultancies for the use of the GRC tool. In this case, there are challenges for the implementation as this can create a further risk that was not considered from the start of the project. The IT basis team of the enterprise should know how to solve the problems that may occur in the future; and train more people while sharing the knowledge about the system. Those principles can make a strong GRC environment within the organization.

'Training the people inside the organization about GRC principles and about the new implemented GRC system is crucial. Once you have them committed with the system, you have people knowing about the tool and you do not rely on external consultancies. That can avoid further risk for your organization' (GRC Expert 1)

There are a lot of problems and challenges that should be considered before implementing a new GRC technology within an organization. However, there are many cases where even if the stakeholders are experienced enough, some problems still exist and the project team should overcome them if they want to achieve a successful outcome. These problems should be identified from their start in order to be solved before they introduce a greater challenge for the whole project.

5 Discussion

The GRC implementation particularities and characteristics as these were identified from the previous sections can be summarized in the following table.

Based on Table 3 and the analysis made in Section 4 we can draw a map of typical characteristics of GRC projects that need to be considered when embarking to a new implementation. As GRC systems are still in their infancy and not well understood by most organizations our results can be used by managers involved in pre, during and post implementation phase of these systems. From a practical perspective, these

Table 3 Characteristics of GRC systems implementation

Characteristics	GRC Systems Implementation
Goals and Objectives	• Strategic financial reporting and controlling
	• Efficient and effective business operations
	• Compliance with the laws and regulations
Purpose of the system	• Risk management, control monitoring and information sharing oriented
Key stakeholders	• Project manager
	• GRC experts
	• Finance team
	• Audit team
	• IT team
	• consultants
	• GRC Systems vendor
	• project team members
Methodologies prior to implementation	• Manual, non-automated frameworks and methodologies or other controlling systems
Requirements prior the implementation (organizational and technical)	• Business case developed–define risk requirements
	• Identification of the risks
	• Identification of the roles and who owns each risk, controls their content and approve those risks
	• Current state analysis- current GRC framework to start with
	• Selection of software and software vendor –IT infrastructure of the organization, the IT landscape (what systems they use)
	• Project plan (how the system will be rolled out, supported, maintained and upgraded)
	• Change management plan
	• Budget planning
	• Decision to proceed the plan
Critical success factors	• Top management support
	• Key stakeholders involved
	• Achieve a common understanding about the need of a GRC solution
	• Cascade information throughout the organization improving various functions
	• Define the GRC system requirements
	• Identification of the process owners and the risks associated with it
	• Training of internal people to be able to manage the system
Problems / Barriers	• The technical complexity of the GRC solutions
	• The company is not ready for a GRC solution
	• There is no control framework already in the organization
	• There are conflicting priorities within the organization
	• A complicated GRC solution that is difficult to work
	• Lack of training of the IT team of the organization on the GRC system

characteristics and the analysis will help enterprises to understand GRC systems and avoid mindless decisions and risks related to problematic implementation processes. Furthermore, they can develop and improve their GRC strategy for their competitive advantage and identify the benefits they can have from their GRC practices.

From a theoretical perspective, the research contributes to the knowledge of GRC systems and their implementation within the enterprises as an effort to bridge the literature gap (Racz et al. 2010b) related to the lack of scientific studies in the area. As GRCs consist a newly developed area of enterprise systems our study is an attempt to gain a better insight of issues related to their implementation including areas currently missing in the existing literature. Our study is addressing previous gaps in the literature by looking at GRCs as systems involving the whole enterprise rather than focusing in one aspect such as accounting (Wiesche et al. 2011). As the current literature on GRC systems, presented in Section 1 and summarized in Table 1, is primarily concerned with the technical/instrumental application of GRC systems this study is advancing the understanding of the true nature of these systems as well as their role in the organizational life.

6 Conclusions

The purpose of this paper is to draw a clearer picture of GRC systems based on the dataset of experts' opinions. The interviews were analysed through the thematic analysis and the key areas were discussed and confirmed by the stakeholders.

Through the investigation of GRC IS aspects with the help of enterprise system theories, the study above has presented a categorization of the characteristics of the GRC IS implementation projects.

Some limitations of the study are typical of the ones met in qualitative studies such as the number of participants as well as the geographical context of the research. These limitations were alleviated to a certain degree by the participants' vast experience in GRC projects in various organizational and geographical settings. These can be addressed in future studies by including views from other organizations/experts and also conduct studies outside Europe. Additionally, future research in the field can use this analysis of the GRC characteristics and investigate further the ways of improving and enhancing the enterprise performance. Another future study can be the identification of possible problem areas of the GRC implementation within the enterprise; and how they can be overcome in order to deliver the best results of GRC projects.

Acknowledgments The authors would like to thank the Editor and the anonymous reviewers for their constructive comments and suggestions for improvement on the earlier versions of this paper. Konstantina Spanaki would like also to acknowledge Grant EP/ K039504/1 from Engineering and Physical Sciences Research Council (EPSRC) which funded part of this research.

References

Ali, S., & Green, P. (2012). Effective information technology (IT) governance mechanisms: an IT outsourcing perspective. *Information Systems Frontiers, 14*(2), 179–193.

Asprion, P. M., & Knolmayer, G. F. (2013). Assimilation of compliance software in highly regulated industries: An empirical multitheoretical investigation. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 4405–4414). New York: IEEE.

Boyatzis, R. E. (1998). *Thematic analysis: Coding as a process for transforming qualitative information*. Thousand Oaks: Sage Publications.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Butler, T., & McGovern, D. (2012). A conceptual model and IS framework for the design and adoption of environmental compliance management systems. *Information Systems Frontiers, 14*(2), 221–235.

Dameri, R. P. (2009). Improving the benefits of IT compliance using enterprise management information systems. *Electronic Journal Information Systems Evaluation Volume, 12*(1), 27–38.

Frigo, M. L., & Anderson, R. J. (2009). A strategic framework for governance, risk, and compliance. *Strategic Finance, 90*(8), 20–61.

Gangadharan, G. R., D'Andrea, V., De Paoli, S., & Weiss, M. (2012). Managing license compliance in free and open source software development. *Information Systems Frontiers, 14*(2), 143–154.

Gericke, A., Fill, H. G., Karagiannis, D., & Winter, R. (2009). Situational method engineering for governance, risk and compliance information systems. In *Proceedings of the 4th international conference on design science research in information systems and technology* (p. 24). New York: ACM.

Gill, S., & Purushottam, U. (2008). Integrated GRC-is your organization ready to move. Governance, risk and compliance. *SETLabs Briefings*, 37–46.

Hoffmann, J., Weber, I. M., & Governatori, G. (2012). On compliance checking for clausal constraints in annotated process models. *Information Systems Frontiers, 14*(2), 155–177.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly, 23*, 67–93.

Ly, L. T., Rinderle-Ma, S., Goeser, K., & Dadam, P. (2012). On enabling integrated process compliance with semantic constraints in process management systems. *Information Systems Frontiers, 14*(2), 195–219.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook*. Thousand Oaks: Sage.

Mitchell, S. L. (2007). GRC360: a framework to help organizations drive principled performance. *International Journal of Disclosure and Governance, 4*(4), 279–296.

Mundy, J., & Owen, C. A. (2013). The use of an ERP system to facilitate regulatory compliance. *Information Systems Management, 30*(3), 182–197.

Nissen, V., & Marekfia, W. (2013). Towards a research agenda for strategic governance, risk and compliance (GRC) management. In *Business Informatics (CBI), 2013 I.E. 15th Conference on* (pp. 1–6). New York: IEEE.

Nissen, V., & Marekfia, W. (2014). The development of a data-centred conceptual reference model for strategic GRC-management. *Journal of Service Science and Management, 7*(02), 63.

OCEG (2007). *Key findings report. The 2007 GRC strategy study*. http://www.oceg.org. Accessed 14 Apr 2010.

Paulus, S. (2009). *A GRC reference architecture. Kuppinger Cole overview report* [Online]. http://www.kuppingercole.com/report/sp_overview_repo_grc_arch_051009. Accessed 25 Nov 2012.

PricewaterhouseCoopers. (2004). *Driven performance: A New strategy for success through integrated governance, risk and compliance management. A white paper*. Frankfurt: PricewaterhouseCoopers International Limited.

Racz, N., Panitz, J.C., Amberg, M., Weippl, E., & Seufert, A. (2010a). *Governance, risk & compliance (GRC) status quo and software use: results from a survey among large enterprises. In ACIS 2010 Proceedings, Paper 21*. http://aisel.aisnet.org/acis2010/21. Accessed 7 May 2011.

Racz, N., Weippl, E., & Seufert, A. (2010b). A frame of reference for research of integrated governance, risk and compliance (GRC). In *Communications and multimedia security* (pp. 106–117). Berlin: Springer Berlin Heidelberg.

Racz, N., Weippl, E., & Seufert, A. (2010c). A process model for integrated IT governance, risk, and compliance management. In J. Barzdins & M. Kirikova (Eds.), *Databases and information systems. Proceedings of the ninth international Baltic conference, Baltic DB&IS 2010* (pp. 155–170). Riga: University of Latvia Press.

Rasmussen, M. (2009). An enterprise GRC framework. *Internal Auditor, 66*(5), pp. 61,63,65.

Sadiq, S., Muehlen, M., & Indulska, M. (2012). Governance, risk and compliance: applications in information systems (editorial). *Information Systems Frontiers, 14*, 123–124.

Scott, S. V., & Perry, N. (2012). The enactment of risk categories: the role of information systems in organizing and re-organizing risk management practices in the energy industry. *Information Systems Frontiers, 14*(2), 125–141.

Spanaki, K., & Papazafeiropoulou, A. (2013). *Analysing the governance, risk and compliance (GRC) implementation process: primary insights. Proceedings of the 21st European conference on information systems (ECIS)*. Utrecht, Netherlands

Strecker, S., Heise, D., & Frank, U. (2011). RiskM: a multi-perspective modeling method for IT risk assessment. *Information Systems Frontiers, 13*(4), 595–611.

Tapscott, D. (2006). *Trust and competitive advantage: an integrated approach to governance, risk & compliance. New Paradigm Learning Corporation* [Online] . http://204.154.71.138/pdf/Trustand-Competitive-Advantage.pdf. Accessed 25 Nov 2012.

Vicente, P., & da Silva, M. M. (2011). A conceptual model for integrated governance, risk and compliance. *Advanced Information Systems Engineering, 6741*, 199–213.

Wiesche, M., Schermann, M., & Krcmar, H. (2011). Understanding the role of information technology for organizational control design: Risk control as new control mechanism. In *Governance and sustainability in information systems. Managing the transfer and diffusion of IT* (pp. 135–152). Berlin: Springer Berlin Heidelberg.

Yu, Y. R., Seo, S. C., & Kim, B. K. (2013). IT GRC-based IT internal control framework. In *Proceedings of the 2013 15th International Conference on Advanced Communication Technology (ICACT)* (pp. 382–385). New York: IEEE.

Dr Anastasia Papazafeiropoulou is a senior lecturer in the computing science department at Brunel University, UK. She has been involved in a number of European and UK funded research projects with emphasis on electronic commerce and small and medium size enterprises (SMEs). She teaches information systems management and business integration at the postgraduate level. She also supervises researchers in the field of technology adoption by organisations with special interest in developing countries. She has 10 years of research experience on the study of diffusion and adoption of electronic commerce, broadband Internet, Enterprise Recourse Planning Systems (ERPs), Customer Relationship Management systems (CRMs), IP-telephony and mobile TV.

Konstantina Spanaki is a Research Associate in the Innovation and Entrepreneurship Group, Imperial College London. Her main research interests lie within the broad area of Information Systems, with a particular focus on enterprise systems, IS adoption, business processes, IT integration and information management intelligence. She received her Ph.D. in Information Systems from Department of Computer Science Brunel University London and a M.Sc. in Information Systems and Management from Warwick Business School. She also holds a B.Sc. in Business Administration (with specialization in Business Information Systems) from Athens University of Economics and Business.